W32.Mydoom.B@mm

--- Mydoom.b ---

Types : Back Door,Covert Proxy,DDoS,Worm
Features : Encrypted,Memory Resident,Persistent
Risk : (Low) Severity : 8.0
Impact 9.1 Contagion Potential 6.8 Wild Low

Aliases

- -------

I-Worm.Mydoom.b, Mydoom.B, W32.Novarg.B@mm, W32/MyDoom-B,

W32/Mydoom.b@MM , Win32.Mydoom.B, WORM_MYDOOM.B

Infection Targets

- -----------------

Microsoft Windows 2000 Advanced Server

Microsoft Windows 2000 Advanced Server SP1

Microsoft Windows 2000 Advanced Server SP2

Microsoft Windows 2000 Advanced Server SP3

Microsoft Windows 2000 Advanced Server SP4

Microsoft Windows 2000 Datacenter Server

Microsoft Windows 2000 Datacenter Server SP1

Microsoft Windows 2000 Datacenter Server SP2

Microsoft Windows 2000 Datacenter Server SP3

Microsoft Windows 2000 Datacenter Server SP4

Microsoft Windows 2000 Professional

Microsoft Windows 2000 Professional SP1

Microsoft Windows 2000 Professional SP2

Microsoft Windows 2000 Professional SP3

Microsoft Windows 2000 Professional SP4

Microsoft Windows 2000 Server

Microsoft Windows 2000 Server SP1

Microsoft Windows 2000 Server SP2

Microsoft Windows 2000 Server SP3

Microsoft Windows 2000 Server SP4

Microsoft Windows 95

Microsoft Windows 95 SR2

Microsoft Windows 98

Microsoft Windows 98SE

Microsoft Windows ME

Microsoft Windows NT Enterprise Server 4.0.0

Microsoft Windows NT Enterprise Server 4.0.0 SP1

Microsoft Windows NT Enterprise Server 4.0.0 SP2

Microsoft Windows NT Enterprise Server 4.0.0 SP3

Microsoft Windows NT Enterprise Server 4.0.0 SP4

Microsoft Windows NT Enterprise Server 4.0.0 SP5

Microsoft Windows NT Enterprise Server 4.0.0 SP6

Microsoft Windows NT Enterprise Server 4.0.0 SP6a

Microsoft Windows NT Server 4.0.0

Microsoft Windows NT Server 4.0.0 SP1

Microsoft Windows NT Server 4.0.0 SP2

Microsoft Windows NT Server 4.0.0 SP3

Microsoft Windows NT Server 4.0.0 SP4

Microsoft Windows NT Server 4.0.0 SP5

Microsoft Windows NT Server 4.0.0 SP6

Microsoft Windows NT Server 4.0.0 SP6a

Microsoft Windows NT Terminal Server 4.0.0

Microsoft Windows NT Terminal Server 4.0.0 SP1

Microsoft Windows NT Terminal Server 4.0.0 SP2

Microsoft Windows NT Terminal Server 4.0.0 SP3

Microsoft Windows NT Terminal Server 4.0.0 SP4

Microsoft Windows NT Terminal Server 4.0.0 SP5

Microsoft Windows NT Terminal Server 4.0.0 SP6

Microsoft Windows NT Workstation 4.0.0

Microsoft Windows NT Workstation 4.0.0 SP1

Microsoft Windows NT Workstation 4.0.0 SP2

Microsoft Windows NT Workstation 4.0.0 SP3

Microsoft Windows NT Workstation 4.0.0 SP4

Microsoft Windows NT Workstation 4.0.0 SP5

Microsoft Windows NT Workstation 4.0.0 SP6

Microsoft Windows NT Workstation 4.0.0 SP6a

Microsoft Windows XP Home

Microsoft Windows XP Home SP1
Microsoft Windows XP Media Center Edition
Microsoft Windows XP Professional
Microsoft Windows XP Professional SP1

Summary
- -------
W32.Mydoom.B@mm is an encrypted mass-mailing worm that arrives as an attachment with either a .exe, .scr, .cmd, .zip, or .pif extension. It also performs a denial of service attack on www.microsoft.com and allows unauthorized remote access to the compromised host.

This worm is currently undergoing analysis. This record will be updated as information becomes available.

Executable Types
- ----------------
File / Binary / Portable Executable (PE)

Infection Vectors
- -----------------
File Transfer / Email Attachment

Impact
- ------
Payload:

Allows unauthorized remote access to the compromised system.

Payload:

Overwrites the HOSTS file making many security and antivirus websites unavailable to the compromised user.

Payload:

Performs a denial of service attack on the website www.microsoft.com or www.sco.com depending on the system date.

Collateral Damage:

Creates a mass-mailing of itself which may clog mail servers or degrade network performance.

Collateral Damage:

Creates a mass-mailing of itself which may impact system performance.

Collateral Damage: Network performance may decrease due to denial of service attacks.

Symptoms

- --------

Creates the following files:

%Temp%\Message

%System%\taskmon.exe

%System%\ctfmon.dll

Creates the following registry entries:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Explorer = %System%\explorer.exe

HKEY_CURRENT_USER\Software\Microsft\Windows\CurrentVersion\Run\Explorer = %System%\explorer.exe

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version

HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32\"(

Default)" = "%System%\ctfmon.dll"

Creates a copy of itself as one of the following filenames in theuser's Kazaa download directory:

xsharez_scanner

BlackIce_Firewall_Enterpriseactivation_crack

zapSetup_95_693

MS59-56_hotfix

winamp0

NessusScan_pro

attackXP-6.71

with one of the following extensions:

pif

scr

bat

Listens on TCP ports 1080, 3128, 80, 8080, or 10080.

Overwrites the HOSTS file.

Scans for other systems listening on TCP port 3127.

Technical Description

- ---------------------

W32.Mydoom.B@mm is an encrypted mass-mailing worm that arrives as a message attachment using either a .exe, .scr, .cmd, or .pif extension. These files may be included as an attached .zip archive. The worm sends itself to all email addresses it locates in files on the system with the following extensions:

.htm

.sht

.php

.asp

.dbx

.tbb

.adb

.pl

.wab

.txt

It will avoid sending itself to addresses in any domain names containing the following strings:

avp

syma

icrosof

msn.

hotmail

panda

sopho

borlan

inpris

example

mydomai

nodomai

ruslis

.gov

gov.

.mil

foo.

berkeley

unix

math

bsd

mit.e

gnu

fsf.

ibm.com
google
kernel
linux
fido
usenet
iana
ietf
rfc-ed
sendmail
arin.
ripe.
isi.e
isc.o
secur
acketst
pgp
tanford.e
utgers.ed
mozilla

It also avoids sending itself to any of the following usernames:

root
info
samples
postmaster
webmaster
noone
nobody
nothing
anyone
someone
your
you

me

bugs

rating

site

contact

soft

no

somebody

privacy

service

help

not

submit

feste

ca

gold-certs

the.bat

page

admin

icrosoft

support

ntivi

unix

bsd

linux

listserv

certific

google

accoun

The worm may spoof the From address of the messages it sends. To do so,

it takes random addresses it gathered above and adds one of the following usernames to the domain name:

sandra

linda

julie
jimmy
jerry
helen
debby
claudia
brenda
anna
alice
brent
adam
ted
fred
jack
bill
stan
smith
steve
matt
dave
dan
joe
jane
bob
robert
peter
tom
ray
mary
serg
brian
jim
maria
leo
jose

andrew
sam
george
david
kevin
mike
james
michael
alex
john

The message may have the following properties:

Subject may include the following:

Returned mail
Delivery Error
Status
Server Report
Mail Transaction Failed
Mail Delivery System
hello
hi

Message Body can be one of the following:
sendmail daemon reported:

Error #804 occured during SMTP session. Partial message has been received.

Mail transaction failed. Partial message is available.

The message contains Unicode characters and has been sent as a binary attachment.

The message contains MIME-encoded graphics and has been sent as a binary attachment.

The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

The attachment may be use one of the following filenames:

document
readme
doc
text
file
data
test
message
body

It may also use a double extension. If it does, the first extension will be one the following:
.htm
.txt
.doc

The attachment will always end with one of the following extensions:
.pif
.scr
.exe
.cmd
.bat
.zip

The icon used may be that of a text file if the extension is .exe or .scr, otherwise it uses the icon of an MS-DOS application.

When the attachment is executed, Notepad will open displaying garbage characters from the file %Temp%\Message dropped by the worm.

Next, it creates the following copy of itself:
%System%\explorer.exe

The worm then creates the following registry entries so that it executes every time Windows starts:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Explorer = %System%\explorer.exe

HKEY_CURRENT_USER\Software\Microsft\Windows\CurrentVersion\Run\Explorer = %System%\explorer.exe

The worm will also modify the following registry entry so that it will be loaded by explorer.exe:
HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32\"(Default)" = "%System%\ctfmon.dll"

The following registry keys are also created:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version

The worm also copies itself to the user's Kazaa downloads directory using one of the following filenames:

xsharez_scanner
BlackIce_Firewall_Enterpriseactivation_crack
zapSetup_95_693
MS59-56_hotfix
winamp0
NessusScan_pro

attackXP-6.71

with one of the following extensions:

pif

scr

bat

If the shimgapi.dll file dropped by W32.Novarg.A@mm is present, the worm will delete it. It then drops the following file:

%System%\ctfmon.dll

This file appears to function as a back door that allows remote access to a compromised host on TCP ports 1080, 3128, 80, 8080, or 10080. Evidence suggests that this back door may also allow the compromised system to be used as a remote proxy.

The worm also appears to be capable of performing a denial of service attack on two distinct websites. If the compromised system date is greater than or equal to Feb 1, 2004, the worm will perform a DoS attack on www.sco.com. During the DoS attack, the worm creates 7 threads that invoke GET requests continuously for the main page of www.sco.com.

However, if the compromised system date is greater than or equal to Feb 3, 2004, the worm performs the DoS attack on www.microsoft.com. During this DoS attack, the worm creates 13 threads that invoke GET requests continuously for the main page of www.microsoft.com.

The worm continues its DoS attack until March 1, 2004.

The worm uses the hostname (i.e. www.sco.com and www.microsoft.com) and not a specific IP.

This variant also overwrites the HOSTS file in order to prevent the user from accessing various websites. Some of the websites include antivirus and security vendors, possibly to prevent the user from obtaining antivirus updates and fix tools. The following entries are added to the HOSTS file:

ad.doubleclick.net
ad.fastclick.net
ads.fastclick.net
ar.atwola.com
atdmt.com
avp.ch
avp.com
avp.ru
awaps.net
banner.fastclick.net
banners.fastclick.net
ca.com
click.atdmt.com
clicks.atdmt.com
dispatch.mcafee.com
download.mcafee.com
download.microsoft.com
downloads.microsoft.com
engine.awaps.net
fastclick.net
f-secure.com
ftp.f-secure.com
ftp.sophos.com
go.microsoft.com
liveupdate.symantec.com
mast.mcafee.com
mcafee.com
media.fastclick.net
msdn.microsoft.com
my-etrust.com
nai.com
networkassociates.com
office.microsoft.com
phx.corporate-ir.net

secure.nai.com
securityresponse.symantec.com
service1.symantec.com
sophos.com
spd.atdmt.com
support.microsoft.com
symantec.com
update.symantec.com
updates.symantec.com
us.mcafee.com
vil.nai.com
viruslist.ru
windowsupdate.microsoft.com
www.avp.ch
www.avp.com
www.avp.ru
www.awaps.net
www.ca.com
www.fastclick.net
www.f-secure.com
www.kaspersky.ru
www.mcafee.com
www.microsoft.com
www.my-etrust.com
www.nai.com
www.networkassociates.com
www.sophos.com
www.symantec.com
www.trendmicro.com
www.viruslist.ru
www3.ca.com

UPDATE: It appears that W32.Mydoom.B@mm scans for systems listening on TCP port 3127. This port is associated with the back door installed by W32.Novarg.A@mm (MCID 2468). If the worm finds a Novarg.A system

listening on TCP port 3127, it will issue commands to terminate the worm and install Mydoom.B on the system.

*UPDATE: A previous conjecture regarding the possible failure of a denial of service routine targeted against www.microsoft.com, due to HOSTS file modifications has been proven false during ongoing analysis. The denial of service routine is fully functional.

Mitigating Strategies

Mass-mailing worms can often originate from people the user knows. Do not open or execute unexpected message attachments.

Filter attachments not on a list of approved types at the e-mail gateway.

Apply the Outlook E-mail Security Update (Q262631) in order to block user access to certain attachment types. This update will also notify the user of applications attempting to access the Outlook address book.

Disinfection

Symantec is not currently aware of any manual disinfection techniques.

Variants

Variant of

W32.Novarg.A@mm

References

Symantec W32.Novarg.A@mm
http://www.symantec.com/avcenter/venc/data/w32.novarg.a@mm.html

McAfee W32/Mydoom@MM http://vil.nai.com/vil/content/v_100983.htm

F-Secure Novarg http://www.europe.f-secure.com/v-descs/novarg.shtml

Computer Associates Win32.Mydoom.A
http://www3.ca.com/virusinfo/virus.aspx?ID=38102

Trend Micro WORM_MIMAIL.R
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MIMA

IL.R

Norman W32/MyDoom.A@mm http://www.norman.com/virus_info/w32_mydoom_a_mm.shtml

Sophos W32/MyDoom-A http://www.sophos.com/virusinfo/analyses/w32mydooma.html

Kaspersky Labs I-Worm.Novarg http://www.avp.ch/avpve/worms/email/novarg.stm

Panda Software Mydoom.A
http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?IdViru

s=44140&sind=0

CERT CERT? Advisory CA-2004-02 Email-borne Viruses
http://www.cert.org/advisories/CA-2004-02.html

McAfee W32/Mydoom.b@MM

http://vil.nai.com/vil/content/v_100988.htm

F-Secure Mydoom.B http://www.europe.f-secure.com/v-descs/mydoom_b.shtml

Trend Micro WORM_MYDOOM.B
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYDO

OM.B

Symantec W32.Mydoom.B@mm
http://www.symantec.com/avcenter/venc/data/w32.mydoom.b@mm.html

Norman W32/MyDoom.B@mm http://www.norman.com/virus_info/w32_mydoom_b_mm.shtml

Computer Associates Win32.Mydoom.B
http://www3.ca.com/virusinfo/virus.aspx?ID=38114

Sophos W32/MyDoom-B http://www.sophos.com/virusinfo/analyses/w32mydoomb.html

* * * * * * * *
Cyber Security Group
NIC